Remarks

Claims 1-4, 6-13, 15, 19-21, 23, 25-30, 33, 37, 39-49 are in the application. Claims 5, 14, 16-18, 22, 24, 31-32, 34-36, and 38 are cancelled. Claims 39-51 are added. Claims 1, 19 and 39 are in independent form. Reconsideration is requested.

Claims 1 and 19 stand rejected for obviousness type double patenting over copending US application No. 10/734,484 ('484 application) in view of US Publication No. 2003/0046447 by Kouperchaliak. Claims 1 and 19 as amended recite memory components and a memory controller that are not recited in the claims of the '484 application or described in Kouperchaliak. Applicant submits, therefore, that claims 1 and 19 are not obvious in view of the cited references and request that the rejection be withdrawn.

1, 5, 9, 11-12, 14-17, 19-20, 24, 27, 29-30, 32-35 stand rejected under 35 USC 103(a) for obviousness over US Publication No. 2003/0087601 of Agam et al. (hereafter Agam) in view of US Publication No. 2003/0046447 of Kouperchaliak et al. (hereafter Kouperchaliak). The remaining claims stand rejected for obviousness over Agam and Kouperchaliak in view of various other references.

The Examiner states that Agam describes the subject matter of original independent claims 1 and 19, but Agam failed to teach a memory component storing autorun software and a computer software application, the autorun software being operable to automatically install and execute the computer software application on a computing device. The Examiner cites Kouperchaliak as disclosing autoplay software and concludes that it would be obvious to combine the autoplay software with the system of Agam. Applicant responds as follows.

Agam is directed to an apparatus for enabling communication between a personal device coupled with a wireless proximity communication interface (e.g., proximity radio signals and infrared signals) and a host computer coupled with a wired communication interface (e.g., USB, RS232, parallel communication). The apparatus includes a wired communication interface, corresponding to the wired communication interface of the host computer, for enabling communication between the apparatus and the host computer; a wireless proximity communication interface, corresponding to the wireless proximity communication interface of the personal device, that includes a controller, for enabling communication between the wired interface of the apparatus and the wireless proximity communication interface of the apparatus. The apparatus further includes a processing means (e.g. a smartcard chip), for performing operations (e.g., encryption, decryption, cipher, ECC, RSA, PKI, DES, MD5 and RC4) such as computing operations (e.g. converting between data that corresponds to the wireless proximity communication interface and data that corresponds to the wired communication interface), secure computing operations, storing data, securely storing data, and so forth.

As described at paragraph [0057] of Agam:

> It should be noted that computational operations performed by the smartcard 70 can be performed also by the microcontroller 40, however microcontrollers are designed for specific operations, while smartcards are designed for a more generic computing purposes. Typically, smartcards comprise API (Application Program Interface), which facilitates the development process. But beyond the programming capability, smartcards also have a major feature that is not common in other type of processors the difficulty of reading their content. Smart cards are designed such that there is a barrier of reading their content. This feature has a major importance in security related applications. For example, storing a PIN within the memory unit of a smartcard is much safer than storing a key within other type of memory.

Accordingly, Agam is directed to using a “smartcard” because it is deemed to be more versatile than a microcontroller. In addition, Agam described using a “smartcard” for securely storing a PIN for use as an entry to an application on the host computer.

Kouperchaliak is directed to providing improved “plug & play” functionality of USB computer peripherals by allowing a USB peripheral to install the drivers needed to operate the peripheral with a host computer. For example, Kouperchaliak describes a printer that has stored on it “device-related software (DRS)” (e.g., software drivers) that permit interaction between the printer and the computer. The printer checks whether device-related software (i.e., drivers) are already installed on the host computer and, if not, uploads the device-related software to the computer for the proper installation and operation of the peripheral device by the computer.

Amended independent claim1 recites a portable wireless communication device that is connectable to a computing device and includes a wireless communication component for enabling wireless radio frequency communication. (See, for example, application paragraph [0037].) A private memory component that includes a private area that is not accessible or viewable by a user, the private memory area storing protected computer software, the protected computer software being installable and executable at the computing device to enable the radio frequency communication at the computing device upon connecting the portable wireless communication device to a computing device. (See, for example, application paragraphs [0044]-[0046] and Figs. 1-5.) Furthermore, the portable wireless communication device launches the protected computer software on the computing device and provides the computing device with wireless Internet access through the wireless communication component. (See, for example, application paragraphs [0019] and [0127].)

With regard to claim 1, the cited art does not teach or suggest a communication component for enabling wireless radio frequency communication, a private memory component includes a private area that is not accessible or viewable by a user, the private memory area storing protected computer software, the protected computer software being installable and executable at the computing device to enable the radio frequency communication at the computing device.

More specifically, Agam, Kouperchaliak, and the other cited references provide no teaching or suggestion of a portable device with private memory component that includes a private area that is not accessible or viewable by a user and that stores protected computer software, which is obtained by the autorun operation for automatic installation on the computing device. Agam describes use of a processing means (e.g. a smartcard chip), for performing operations (e.g., encryption, decryption, cipher, ECC, RSA, PKI, DES, MD5 and RC4) such as computing operations (e.g. converting between data that corresponds to the wireless proximity communication interface and data that corresponds to the wired communication interface), secure computing operations, storing data, securely storing data, and so forth. The secure storing of data refers to storing just a PIN within the memory unit of a smartcard for increased security. Agam provides no teaching or suggestion of storing protected computer software in a secure manner.

Likewise, Kouperchaliak describes a peripheral device (e.g., a printer) operable to install onto a computer device-related software (e.g., a printer driver) that stored in the memory of the peripheral device. The memory 38 of Kouperchaliak is described as being “a non-volatile memory such as ROM, PROM or flash memory.” Nothing in Kouperchaliak teaches or suggests storing protected computer software in a secure manner. Applicant submits, therefore that claim 1 is patentably distinct and allowable over the cited art in view of the private memory component that includes a private area that is not accessible or viewable by a user and that stores protected computer software, which is obtained by the autorun operation for automatic installation on the computing device.

Furthermore, the cited references provide no teaching or suggestion of automatically installing and launching protected computer software on a computing device and to provide the computing device with wireless Internet access through a wireless communication component. Agam is directed to providing Wireless Proximity Communication (i.e., local wireless communication) between a personal device and a local host computer. Kouperchaliak is directed to installing a driver for a peripheral device, such as a printer. Neither Agam nor the other references is directed to installing and launching protected computer software on a computing device to provide the computing device with wireless Internet access through a wireless communication component. For this and the foregoing reasons, applicant submits that claim 1 and its dependent claims are patentably distinct from the cited references.

Similarly to claim 1, amended claim 19 recites a portable wireless communication device connectable to a computing device with a wireless communication component for enabling wireless radio frequency communication. A memory component has a public area that is accessible and viewable by a user for storage and a private area that is not accessible or viewable by the user, the private area storing therein a protected computer software application that is operable to be automatically installed and executed on the computing device upon connecting the device interface to the external interface of the computing device, thereby to provide the computing device with wireless Internet access through the wireless communication component. A memory controller manages communication through the device interface and accesses the memory component that includes the private area.

With regard to claim 19, the cited art does not teach or suggest a wireless communication component for enabling wireless radio frequency communication, a memory component that has a public area that is accessible and viewable by a user for storage and a private area that is not accessible or viewable by the user, the private area storing therein a protected computer software application that is operable to be automatically installed and executed on the computing device upon connecting the device interface to the external interface of the computing device to provide the computing device with wireless Internet access through the wireless communication component, and a memory controller that manages communication through the device interface and accesses the memory component that includes the private area.

More specifically, Agam, Kouperchaliak, and the other cited references provide no teaching or suggestion of a memory component that has a public area that is accessible and viewable by a user for storage, and a private area that is not accessible nor viewable by the user, the private area storing therein a protected computer software application that is operable to be automatically installed and executed on the computing device upon connecting the device interface to the external interface of the computing device. Agam describes use of a processing means (e.g. a smartcard chip), for performing operations (e.g., encryption, decryption, cipher, ECC, RSA, PKI, DES, MD5 and RC4) such as computing operations (e.g. converting between data that corresponds to the wireless proximity communication interface and data that corresponds to the wired communication interface), secure computing operations, storing data, securely storing data, and so forth. The secure storing of data refers to storing just a PIN within the memory unit of a smartcard for increased security. Agam provides no teaching or suggestion of storing a protected computer software application in a secure manner.

Likewise, Kouperchaliak describes a peripheral device (e.g., a printer) operable to install onto a computer device-related software (e.g., a printer driver) that stored in the memory of the peripheral device. The memory 38 of Kouperchaliak is described as being “a non-volatile memory such as ROM, PROM or flash memory.” Nothing in Kouperchaliak teaches or suggests storing protected computer software in a secure manner. Applicant submits, therefore that claim 19 is patentably distinct and allowable over the cited art in view of the memory component that has a public area that is accessible and viewable by a user for storage, and a private area that is not accessible nor viewable by the user, the private area storing therein a protected computer software application that is operable to be automatically installed and executed on the computing device upon connecting the device interface to the external interface of the computing device.

As noted above, neither Agam nor Kouperchaliak teaches or suggests a private area that is not accessible or viewable by the user, the private area storing therein a protected computer software application that is operable to be automatically installed and executed on the computing device. Accordingly, neither Agam nor Kouperchaliak teaches or suggests a memory controller that manages communication with a device interface and accesses the memory component that includes the private area and the computer software application is automatically installed and executed on the computing device upon connecting the device interface to the external interface of the computing device.

Moreover, Kouperchaliak describes a mass storage device emulator that is turned on to perform an autoplay operation by a functional switch 36 if the driver for the peripheral device has not previously been installed:

> Upon starting the peripheral device, which generally occurs when the peripheral device is plugged in, the function switch 36 automatically switches the peripheral device over to the mass storage device emulator. The peripheral device therefore initially registers with the operating system as a mass storage device such as a CD device (step 50). The device-related software, if installed, either automatically sends out device-related software identification strings, or replies to the peripheral devices request for the identification strings, with the intention of obtaining the acknowledgement of the requesting device Thus strings received are intercepted at the mass storage device emulator port and read If (step 52) the device-related software identification string corresponding to the peripheral device of the invention is identified, then the peripheral device knows that the appropriate device-related software is installed on the computer The mass storage device emulator 34 is disconnected (step 66) and the functional module 32 is connected in its place (step 68) for normal operation of the peripheral device. Kouperchaliak, paragraph [0041].

Hence, Kouperchaliak describes a mass storage device emulator 34 that is turned on to provide the Autoplay operation, and is otherwise turned off. Neither Kouperchaliak nor any of the other references teaches or suggests a memory controller that manages communication with a device interface and accesses the memory component that includes the private area where the protected computer software application is automatically installed and executed on the computing device. Applicant submits, therefore that claim 19 is patentably distinct and allowable over the cited art in view of the recited memory controller that manages communication with a device interface and accesses protected computer software from a private memory area.

Furthermore, the cited references provide no teaching or suggestion of automatically installing and executing on the computing device a protected computer software application to provide the computing device with wireless Internet access through a wireless communication component. Agam is directed to providing Wireless Proximity Communication (i.e., local wireless communication) between a personal device and a local host computer. Kouperchaliak is directed to installing a driver for a peripheral device, such as a printer. Neither Agam nor the other references is directed to installing and executing a protected computer software application on a computing device to provide the computing device with wireless Internet access through a wireless communication component. For this and the foregoing reasons, applicant submits that claim 19 and its dependent claims are patentably distinct from the cited references.

Added independent claim 39 is directed to a portable wireless communication device subcombination that includes a USB device interface, a hub, and a memory controller having a processor that is executable to manage communication with the hub and the USB interface, facilitate an autorun operation for automatically launching and installing on the computing device the protected computer software upon connecting the USB interface to the computing device, and access the protected computer software in the private area of the memory component. Features of claim 39 are illustrated and described with reference to Fig. 4, for example. Claim 39 recites features that are described above with reference to claims 1 and 19, including a private memory component and a memory controller that access the private memory component and is functional to manage communication and facilitate an autorun operation. Applicant submits that new claim 39 and its dependent claims are allowable for the reasons set forth above with reference to claims 1 and 19.

Applicant believes the application is in condition for allowance and respectfully requests the same.

IPSOLON LLP
111 SW COLUMBIA #710
PORTLAND, OREGON 97201
TEL. (503) 249-7066
FAX (503) 249-7068

Respectfully Submitted,

/Mark M. Meininger/

Mark M. Meininger
Registration No. 32,428